CLAIMS

What is claimed is:

1. A method for bootstrapping a secure communications channel between devices, comprising:

generating a key via a first device;

establishing a short range communication channel between the first device and a second device;

sending a copy of the key from the first device to the second device via the short range communication channel to produce a shared key that is shared by both the first and second devices;

establishing a secure communication channel between the first and second devices using an encrypted communication protocol that implements an encryption scheme based on a common encryption key derived from the shared key, said secure communication channel being separate and apart from the short range communication channel.

2. The method of claim 1, further comprising sending identity information used to identify the first device from the first device to the second device, wherein the identity information is used to establish the secure communication channel.

3. The method of claim 1, further comprising disabling the short range communication channel after the copy of the key has been sent from the first device to the second device.

4. The method of claim 1, wherein the shared key comprises a cryptographically secure pseudo-random number.

5. The method of claim 1, wherein each of the first and second devices include an authenticated key agreement algorithm software component that is used to cooperatively generate the common encryption key.

6. The method of claim 1, wherein the short range communication channel comprises a transponder/transponder reader pair and wherein the transponder is operatively coupled to the first device and the transponder reader is operatively coupled to the second device.

7. The method of claim 6, wherein the transponder reader is coupled to an antenna that radiates radio frequency (RF) energy that is used to energize the transponder, further comprising waving the transponder in front of or placing the transponder in proximity to the transponder reader to energize the transponder and cause the transponder to transmit data pertaining to the key to enable the data to be read by the transponder reader via the antenna.

8. The method of claim 1, wherein the common cryptographic key is the shared key.

9. The method of claim 1, further comprising performing a peer-to-peer authentication using symmetric authenticated key agreement algorithms running on both devices and the shared key.

10. The method of claim 9, wherein the peer-to-peer authentication is implemented by performing the operations of:

storing credentials data including at least the shared key on both the first and second devices;

generating a first random string with the first device and passing the first random string to the second device;

generating a first digital signature corresponding to the first random string with the first device using an encryption key derived from the credentials data stored on the first device and a symmetric authenticated key agreement algorithm running on the first device;

generating a second digital signature corresponding to the first random string with the second device using an encryption key derived from the credentials data stored on the second device and a symmetric authenticated key agreement algorithm running on the second device;

comparing the first and second digital signatures to see if they match; and

authenticating the second device with the first device if there is a match.

11. The method of claim 10, wherein the peer-to-peer authentication further comprises performing the operation of:

generating a second random string with the second device and passing the second random string to the first device;

generating a third digital signature corresponding to the second random string with the second device using an encryption key derived from the credentials data stored on the second device and a symmetric authenticated key agreement algorithm running on the second device;

generating a fourth digital signature corresponding to the second random string with the first device using an encryption key derived from the credentials data stored on the first device and a symmetric authenticated key agreement algorithm running on the first device;

comparing the third and fourth digital signatures to see if they match; and

authenticating the first device with the second device if there is a match.

12. A method for bootstrapping a secure communications channel between devices, comprising:

generating a key via a first device;

activating a transponder reader in a second device;

transmitting data corresponding to a copy of the key from a transponder operatively coupled to the first device to the transponder reader;

storing the copy of the key in the second device to produce a shared key that is shared by both the first and second devices;

establishing a secure communication channel between the first and second devices using an encrypted communication protocol that implements an encryption scheme based on a common encryption key derived from the shared key.

13. The method of claim 12, further comprising disabling at least one of the transponder and transponder reader after the copy of the key has been sent from the first device to the second device.

14. The method of claim 12, wherein the transponder reader is coupled to an antenna that radiates radio frequency (RF) energy that is used to energize the transponder, further comprising waving the transponder in front of or placing the

transponder in proximity to the transponder reader to energize the transponder and cause the transponder to transmit a signal containing the data corresponding to the copy of the key to enable the data to be read by the transponder reader via the antenna.

15. The method of claim 14, wherein the transponder reader further transmits data via the antenna requesting the transponder to send data to the transponder reader and the transponder sends the data corresponding to the copy of the key in response to receiving the request.

16. The method of claim 12, wherein the transponder comprises a transceiver that sends and receives data using a 13.56 MHz radio frequency signal.

17. A device comprising:

a processor;

a transceiver to receive and send data via radio frequency RF signals;

a key generator operatively coupled to the transceiver and the processor;

a communication interface to send and receive data from an external device via a communication link; and

a memory coupled to the processor in which a plurality of machine instructions including an authenticated key agreement algorithm module are stored that when executed by the processor performs the operations of:

invoking the key generator to generate a key;

passing a copy of the key to the transceiver;

enabling the transceiver to send a copy of the key to the external device via a first RF signal to share the key between the device and the external device; and establishing a secure communication channel with the second device over the communication link that uses a cryptographic key that is generated through execution of the authenticated key agreement algorithm module in cooperative interaction with a symmetrical key agreement algorithm operating on the external device and is based on the key that is shared between the device and the external device.

18. The device of claim 17, wherein the transceiver comprises a transponder that transmits the first RF signal containing data corresponding to the copy of the key in response to receiving a second RF signal containing a data request from the external device.

19. The device of claim 18, wherein the transponder is energized to transmit the first RF signal by receiving RF energy via the second RF signal sent by the external device.

20. The device of claim 17, further comprising a user interface control, coupled to the processor, to receive a user request to establish a secure communication channel between the device and the external device.

21. The device of claim 17, further comprising a persistent memory device in which a device identifier is stored, and wherein execution of the machine instructions by the processor further performs the operation of sending data corresponding to the device identifier to the external device via the first RF signal.

22. A device comprising:

a processor;

a transceiver to receive and send data via radio frequency (RF) signals;

a communication interface to send data to and receive data from an external device via a communication link; and

a memory coupled to the processor in which a plurality of machine instructions including an authenticated key agreement algorithm module are stored that when executed by the processor performs the operations of:

controlling the transceiver to enable the transceiver to receive a copy of a shared key from the external device via a first RF signal; and

establishing a secure communication channel with the external device over the communication link, wherein the secure communication channel uses a cryptographic key that is generated through execution of the authenticated key agreement algorithm module through cooperative interaction with a symmetrical key agreement algorithm operating on the external device and is based on the shared key.

23. The device of claim 22 wherein the transceiver comprises a transponder reader to receive an RF signal generated by a compatible transponder that is operatively coupled to the external device.

24. The device of claim 23, further comprising an antenna coupled to the transponder reader and driven by the transponder reader to generate an RF signal including RF energy that is received by the compatible transponder to energize the compatible transponder.

25. The device of claim 22, further comprising a user interface control, coupled to the processor, to receive a user request to establish a secure communication channel between the device and the external device.